

CRYPTOGRAPHY-BASED TAMPER-RESISTANT

SOFTWARE DESIGN MECHANISM

ABSTRACT OF THE DISCLOSURE

An arrangement is provided for tamper-resistant software to protect high-security data. In an embodiment, high-security authorization information is encrypted using a fingerprint that is computed based on a protected portion of a data access program. When the program is executed, a runtime fingerprint is computed based on the protected portion of the program to decrypt the high-security authorization information. Access to the the high-security data is allowed only when the decryption is successful.

TOP SECRET//SI//FOUO